

**CLAIMS:**

What is claimed is:

1. A method, in a computer system, for monitoring data sent from a computer, comprising:

5           detecting a request for an outgoing transfer of data from a program in the computer system to a destination; determining whether the destination is a trusted site; and performing a corrective action if the destination is

10          not a trusted site.

2. The method of claim 1, wherein the step of determining whether the destination is a trusted site comprises matching the destination against a list of trusted sites.

15 3. The method of claim 1, wherein the corrective action comprises blocking the outgoing transfer.

4. The method of claim 1, wherein the corrective action comprises disabling the program.

5. The method of claim 1, wherein the step of

20 performing a corrective action comprises:

          changing the destination of the outgoing transfer to the computer system; and determining whether the program operates in response to the changed destination.

6. The method of claim 1, wherein the step of performing a corrective action comprises:

irreversibly encrypting the data; and

determining whether the program operates in response

5 to the encryption.

7. The method of claim 6, wherein the step of irreversibly encrypting the data comprises injecting random numbers into the data.

8. The method of claim 1, further comprising:

10 determining whether the amount of data for the outgoing transfer is uncharacteristically high; and

performing a corrective action if the amount of data is uncharacteristically high.

9. The method of claim 1, further comprising:

15 determining whether the data includes personal information; and

performing a corrective action if the data includes personal information.

10. The method of claim 9, wherein the step of

20 determining whether the data includes personal information comprises performing a text string search or binary pattern search on the data.

11. The method of claim 1, wherein the step of

25 performing a corrective action comprises storing a log of the outgoing transfer.

12. The method of claim 11, wherein the step of storing a log of the outgoing transfer comprises storing the data.

13. The method of claim 11, further comprising  
5 transferring the log to a remote computer.

14. A method, in a computer system, for monitoring data sent from a computer, comprising:

detecting a request for an outgoing transfer of data from a program in the computer system to a destination;

10 determining whether the amount of the data is uncharacteristically high; and

performing a corrective action if the amount of the data is uncharacteristically high.

15. The method of claim 14, wherein the corrective  
15 action comprises blocking the data transfer.

16. The method of claim 14, wherein the corrective action comprises disabling the program.

17. The method of claim 14, wherein the step of performing a corrective action comprises:

20 changing the destination of the outgoing transfer to the computer system; and

determining whether the program operates in response to the changed destination.

18. The method of claim 14, wherein the step of performing a corrective action comprises:

irreversibly encrypting the data; and

determining whether the program operates in response

5 to the encryption.

19. The method of claim 18, wherein the step of irreversibly encrypting the data comprises injecting random numbers into the data.

20. The method of claim 14, further comprising:

10 determining whether the data includes personal information; and

performing a corrective action if the data includes personal information.

21. The method of claim 20, wherein the step of

15 determining whether the data includes personal information comprises performing a text string search or binary pattern search on the data.

22. The method of claim 14, wherein the step of

performing a corrective action comprises storing a log of  
20 the outgoing transfer.

23. The method of claim 22, wherein the step of storing a log of the outgoing transfer comprises storing the data.

24. The method of claim 22, further comprising

25 transferring the log to a remote computer.

25. An apparatus for monitoring data sent from a computer system, comprising:

detection means for detecting a request for an outgoing transfer of data from a program in the computer system to a destination;

determination means for determining whether the destination is a trusted site; and

correction means for performing a corrective action if the destination is not a trusted site.

10 26. The apparatus of claim 25, wherein the determination means comprises means for matching the destination against a list of trusted sites.

27. The apparatus of claim 25, wherein the corrective action comprises blocking the outgoing transfer.

15 28. The apparatus of claim 25, wherein the corrective action comprises disabling the program.

29. The apparatus of claim 25, wherein the correction means comprises:

means for changing the destination of the outgoing transfer to the computer system; and

means for determining whether the program operates in response to the changed destination.

30. The apparatus of claim 25, wherein the correction means comprises:

    encryption means for irreversibly encrypting the data; and

5       means for determining whether the program operates in response to the encryption.

31. The apparatus of claim 30, wherein the encryption means comprises means for injecting random numbers into the data.

10 32. The apparatus of claim 25, further comprising:

    means for determining whether the amount of data for the outgoing transfer is uncharacteristically high; and

    means for performing a corrective action if the amount of data is uncharacteristically high.

15 33. The apparatus of claim 25, further comprising:

    means for determining whether the data includes personal information; and

    means for performing a corrective action if the data includes personal information.

20 34. The apparatus of claim 33, wherein the means for

determining whether the data includes personal

information comprises means for performing a text string search or binary pattern search on the data.

35. The apparatus of claim 25, wherein the step of

25 performing a corrective action comprises storage means for storing a log the outgoing transfer.

36. The apparatus of claim 35, wherein the storage means comprises means for storing the data.

37. The apparatus of claim 35, further comprising means for transferring the log to a remote computer.

5 38. An apparatus for monitoring data sent from a computer system, comprising:

detection means for detecting a request for an outgoing transfer of data from a program in the computer system to a destination;

10 determination means for determining whether the amount of the data is uncharacteristically high; and

correction means for performing a corrective action if the amount of the data is uncharacteristically high.

39. The apparatus of claim 38, wherein the corrective

15 action comprises blocking the data transfer.

40. The apparatus of claim 38, wherein the corrective action comprises disabling the program.

41. The apparatus of claim 38, wherein the correction means comprises:

20 means for changing the destination of the outgoing transfer to the computer system; and

means for determining whether the program operates in response to the changed destination.

42. The apparatus of claim 38, wherein the correction means comprises:

    encryption means for irreversibly encrypting the data; and

5       means for determining whether the program operates in response to the encryption.

43. The apparatus of claim 42, wherein the encryption means comprises means for injecting random numbers into the data.

10 44. The apparatus of claim 38, further comprising:

    means for determining whether the data includes personal information; and

    means for performing a corrective action if the data includes personal information.

15 45. The apparatus of claim 44, wherein the means for determining whether the data includes personal information comprises means for performing a text string search or binary pattern search on the data.

46. The apparatus of claim 38, wherein the correction

20 means comprises storage means for storing a log the outgoing transfer.

47. The apparatus of claim 48, wherein the storage means comprises means for storing the data.

Docket No. AUS920010299US1

48. The apparatus of claim 48, further comprising means for transferring the log to a remote computer.

49. A computer program product, in a computer readable medium, for monitoring data sent from a computer system,  
5 comprising:

instructions for detecting a request for an outgoing transfer of data from a program in the computer system to a destination;

10 instructions for determining whether the destination is a trusted site; and

instructions for performing a corrective action if the destination is not a trusted site.

50. A computer program product, in a computer readable medium, for monitoring data sent from a computer system,  
15 comprising:

instructions for detecting a request for an outgoing transfer of data from a program in the computer system to a destination;

20 instructions for determining whether the amount of the data is uncharacteristically high; and

instructions for performing a corrective action if the amount of the data is uncharacteristically high.

PCT/US2001/0299US1